

# Operational Technology Defender Fellowship Program



## Overview

Protecting the nation's energy infrastructure from evolving threats is critical to our national security. Security managers play a decisive role in defending the energy sector against cyber-enabled sabotage and physical security breaches, ranging from storm surges to kinetic attacks. Their work bridging executive intent and technical reality is both critical and challenging — and the necessary resources are often limited.

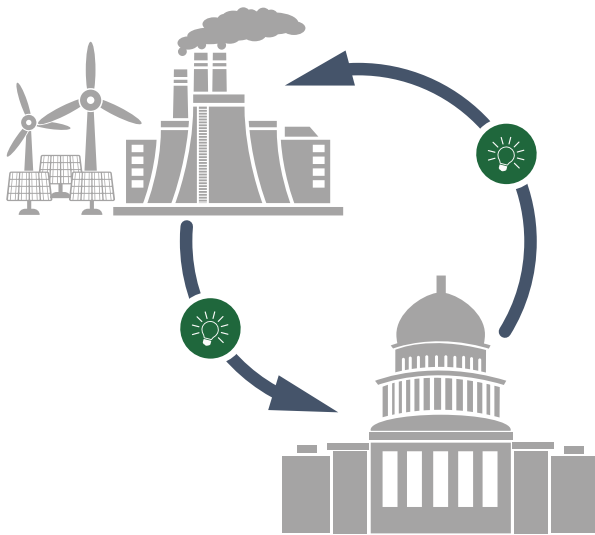
Based on the recommendations of the U.S. Cyberspace Solarium Commission, and to better support these front-line managers, the U.S. Department of Energy's (DOE) Office of Cybersecurity, Energy Security, and Emergency Response (CESER) created the Operational Technology (OT) Defender Fellowship. This training offers middle to senior-level OT security managers in the U.S. energy sector an opportunity to understand the

## Sponsorship

The fellowship is sponsored by DOE and hosted by Idaho National Laboratory (INL), with support from Foundation for Defense of Democracies' Center on Cyber and Technology Innovation.

cyber strategies as well as the tactics, techniques, and procedures adversarial state and nonstate actors use in targeting U.S. energy infrastructure.

## Fellowship Goals



Serve as an information and idea exchange platform between government and energy sector experts, contributing to the bi-directional advancement of improved cybersecurity and information sharing capabilities and processes.

&

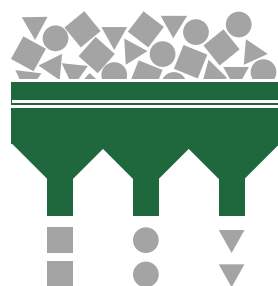
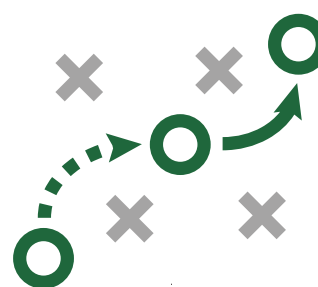


Familiarize and discuss the current state of cybersecurity operations, capabilities, gaps, constraints, and areas for mutual improvement to better defend our nation's critical energy infrastructure.

## Fellowship Objectives

At the conclusion of the OT Defender Fellowship, success will be measured by accomplishing the following objectives:

<https://inl.gov/otdefender/>



## Other OT Related Training Programs

### *CyberStrike Workshop*

To reduce the consequences of cyber-enabled sabotage, DOE-CESER, in collaboration INL, developed the CyberStrike training program. This program works to enhance the ability of energy sector owners and operators to prepare for a cyber incident impacting operational technology.

The training is a unique opportunity for OT Fellows to both attack and defend the equipment used in a utility on a daily basis, leveraging insights from a real-world cyber-attack. The training offers participants a technical understanding of cyber-attacks from the information gathering phase to the impact phase to enhance their ability to defend critical energy infrastructure from adversarial cyber operations.